Notice of Allowability	Application No.	Applicant(s)	
	09/698,159	GHOSH ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *31 July 2006*.

2. ☒ The allowed claim(s) is/are *23-30,33-44 and 47-50 (renumbered as 1-24 respectively)*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☒ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☒ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *11 October 2006* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/11/06

1. In response to amendment filed on 31 July 2006 and Interview on 11 October 2006, the amendment to the claims is accepted.

2. An examiner's amendment to the record is attached. Please enter entire claim set. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. The examiner's amendment to amends claims 23 and 37; was authorized by attorney of record Lawrence D. Eisen in phone interview on 11 October 2006.

Reasons for Allowance

3. Claims 23-30, 33-44, and 47-50 are allowed over the prior art of record.

The following is a statement of reasons for the indication of allowable subject matter:

In interpreting the claims in light of the specification and applicant's argument, the Amendment filed 7/31/2006, as well as attached Examiner's Amendment. Examiner finds the claimed invention is patentable distinct from the prior art of record.

The prior arts of record, Munson introducing a dynamic intrusion detection system, Botros introducing a method for training neural network models for use in a intrusion detection system.

The prior art of record, Munson or Botros fail to anticipate or render Applicant's particular feature that

> **"and based upon a machine learning algorithm, wherein the machine learning algorithm employs a string distance metric, other than string matching, for preprocessing its inputs during learning, wherein a string is defined as a sequence of symbols and string distance metric is based on at least one of events common to two**

strings and the difference in positions of common events, and the string distance metric is used to measure the distance from an input string to each of several exemplar strings"

The dependent claims, being further limiting to the independent claims, defined and enabled by the Specification are also allowed.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 8:30 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen. Tran
Patent Examiner
Technology Center 2134
03 October 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/11/06

EXAMINER'S AMENDMENT:

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1 – 22 Canceled

23. (Currently Amended) A detection system for detecting intrusive behavior in a session on a computer during an application monitoring phase, said session comprising a plurality of applications invoked on said computer, and said computer having a computer operating system, said detection system comprising:

(a) a plurality of trained neural networks, wherein each trained neural network has previously been trained during a training phase to identify a pre-determined behavior pattern for a corresponding one of the plurality of applications, and wherein each trained neural network is selected for use in the application monitoring phase based upon performance during a testing phase and based upon a machine learning algorithm, wherein the machine learning algorithm employs a string distance metric, other than string matching, for preprocessing its inputs during learning, wherein a string is defined as a sequence of symbols and the string distance metric is based on at least one of events common to two strings and/~~or~~ the difference in positions of common events, and the string distance metric is used to measure the distance from an input string to each of several exemplar strings;

(b) a plurality of application profiles, wherein each application profile comprises a plurality of application data for a corresponding one of the plurality of applications, wherein said application data is collected during the session;

(c) a temporal locality identifier, wherein when one of the plurality of application profiles is sequentially input to a corresponding one of the plurality of trained neural networks the trained neural network outputs a behavior indicator for each of the plurality of data strings in the application profile; and wherein if the behavior indicator meets a pre-determined criteria, a counter is incremented, and wherein if the counter has a high rate of increase the temporal locality identifier labels the application behavior intrusive, and wherein if a predetermined percentage of application behaviors are intrusive the session behavior is labeled intrusive.

24. (Original) The detection system of claim 23, wherein the pre-determined behavior pattern comprises a non-intrusive behavior.

25. (Previously Presented) The detection system of claim 23, wherein the application data comprises a distance between a sequential mapping of system calls made by a corresponding one of the plurality of applications and a pre-defined string of system calls.

26. (Previously Presented) The detection system of claim 23, wherein the application data comprises a distance between a sequential mapping of object requests made by a corresponding one of the plurality of applications and a pre-defined string of object requests.

27. (Original) The detection system of claim 23, wherein the plurality of application profiles is created by a data pre-processor application.

28. (Original) The detection system of claim 27, wherein the data pre-processor receives input from an auditing system integral to the computer operating system.

29. (Original) The detection system of claim 27, wherein the data pre-processor creates the plurality of second application profiles in real-time.

30. (Original) The detection system of claim 27, wherein the plurality of trained neural networks receive input from the plurality of application profiles in real-time.

31. (Canceled)

32. (Canceled)

33. (Previously Presented) The detection system of claim 23, wherein the plurality of trained neural networks comprises a plurality of backpropogation neural networks.

34. (Previously Presented) The detection system of claim 33, wherein each backpropogation neural network in the plurality of backpropogation neural networks comprises an input layer, a hidden layer and an output layer.

35. (Previously Presented) The detection system of claim 34, wherein a number of nodes in the hidden layer is determined by testing a plurality of cases for each backpropogation neural network in the plurality of backpropogation neural networks and selecting the backpropogation neural network having a highest accuracy rate during the testing phase for use in application monitoring.

36. (Previously Presented) The detection system of claim 23, wherein the plurality of trained neural networks comprises a plurality of recurrent neural networks.

37. (Currently Amended) A method for detecting intrusive behavior in a session on a computer during an application monitoring phase, said session comprising a plurality of applications invoked on said computer, and said computer having a computer operating system, said method comprising the steps of:

(a) training a plurality of neural networks during a training phase, wherein each neural network is trained to identify a pre-determined behavior pattern for a corresponding one of the plurality of applications;

(b) selecting for use one or more trained neural networks based upon performance during a testing phase and based upon a machine learning algorithm, wherein the machine learning algorithm employs a string distance metric, other than string matching, for preprocessing its inputs during learning, wherein a string is defined as a sequence of symbols and the string distance metric is based on at least one of events common to two strings and/~~or~~ the difference in positions of common events, and the string distance metric is used to measure the distance from an input string to each of several exemplar strings;

(c) creating a plurality of application profiles, wherein each application profile comprises a plurality of application data for a corresponding one of the plurality of applications, wherein said application data is collected during the session;

(d) performing a temporal locality identifying algorithm, wherein when one of the plurality of application profiles is sequentially input to a corresponding one of the plurality of trained neural networks the trained neural network outputs a behavior indicator for each of the plurality of data strings in the application profile, and wherein if the behavior indicator meets a pre-determined criteria, a counter is incremented, and wherein if the counter has a high rate of increase the temporal locality identifier labels the application behavior intrusive, and wherein if a predetermined percentage of application behaviors are intrusive the session behavior is labeled intrusive.

38. (Original) The method of claim 37, wherein the pre-determined behavior pattern comprises a non-intrusive behavior.

39. (Previously Presented) The method of claim 37, wherein the application data comprises a distance between a sequential mapping of system calls made by a corresponding one of the plurality of applications and a pre-defined string of system calls.

40. (Previously Presented) The method of claim 37, wherein the application data comprises a distance between a sequential mapping of object requests made by a corresponding one of the plurality of applications and a pre-defined string of object requests.

41. (Original) The method of claim 37, wherein the plurality of application profiles is created by a data pre-processor application.

42. (Original) The method of claim 41, wherein the data pre-processor receives input from an auditing system integral to the computer operating system.

43. (Original) The method of claim 41, wherein the data pre-processor creates the plurality of second application profiles in real-time.

44. (Original) The method of claim 41, wherein the plurality of trained neural networks receive input from the plurality of application profiles in real-time.

45. (Canceled)

46. (Canceled)

47. (Previously Presented) The method of claim 37, wherein the plurality of trained neural networks comprises a plurality of backpropogation neural networks.

48. (Previously Presented) The method of claim 37, wherein each backpropogation neural network in the plurality of backpropogation neural networks comprises an input layer, a hidden layer and an output layer.

49. (Previously Presented) The method of claim 48, wherein a number of nodes in the hidden layer is determined by testing a plurality of cases for each backpropogation neural network in the plurality of backpropogation neural networks and selecting the case wherein the corresponding neural network has a highest accuracy rate.

50. (Previously Presented) The method of claim 37, wherein the plurality of trained neural networks comprises a plurality of recurrent neural networks.